

21 October 2009

By: Marius Oiaga, Technology News Editor

Windows Vista
Microsoft

[Pirated Vista Black Edition ISO Infected with Malware](#)

Warns Microsoft

The fact that attackers were using [infected pre-release copies of Windows 7](#) to spread their malware to unsuspecting users is simply an example of the most recent releases of the Windows client being turned into vessels for malicious code. Fact is that pre-release versions of [Office 2010 were also infested with malware](#), under a similar malicious code distribution model. However, this practice is not new to Windows 7 and Office 2010. Microsoft has warned that one of the most notorious pirated editions of Windows Vista is also infected with malware and that it will compromise the systems of users looking to grab a free copy of Windows 7's predecessor from torrent trackers or warez websites.

"After MSE's release, we've seen a spike in a particular variant of Win32/Bifrose - Backdoor:Win32/Bifrose.EO. Why, you ask? Well, it seems that the malware authors (or perhaps an unsuspecting pirate) are distributing a 'cracked' version of Windows that comes pre-infected for your convenience - labelled, fittingly, "Vista Black Edition". Just to clarify, this means computer users are downloading an ISO of pirated Microsoft software (and saving to disk on a Genuine Windows system) and a free Microsoft anti-virus product is alerting them to a potential infection in their freshly stolen software. I'm not really sure if 'irony' really emphasises the situation enough. But hey, at least the Windows is free, right?" asked [Matt McCormack](#), from MMPC Melbourne.

Win32/Bifrose - Backdoor:Win32/Bifrose.EO, is, as the moniker implies, a backdoor. In itself, Bifrose will not cause much damage to a machine, outside of switching off Windows Firewall. However, once it has compromised a machine the backdoor will communicate with servers under the control of its author and download additional pieces of malware. McCormack underlines the dangers of "free but pirated" products, especially in the context in which the fact that a piece of software is infested with malware does in no way deter end users from attempting to run it.

"Underground forums are teeming with helpful hints on how to disinfect your newly acquired (though somewhat 'not as advertised') software. No doubt some of the instructions include using other pirated software products," McCormack noted. "'Free' may be changed at any time to actually mean 'cost you', with one or more of the following words appended to the end: passwords, bandwidth, login information, bank account details, email accounts, credit rating, dignity," he added.